



## Privacy Threshold Analysis

Version number: 03-2020

Page 1 of 14

### PRIVACY THRESHOLD ANALYSIS (PTA)

This form will be used to determine whether a Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other privacy compliance documentation is required under the E-Government Act of 2002, the Homeland Security Act of 2002, the Privacy Act of 1974, or DHS policy.

**Please complete this form and send it to your Component Privacy Office.** If you are unsure of your Component Privacy Office contact information, please visit <https://www.dhs.gov/privacy-office-contacts>. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance  
DHS Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
202-343-1717

PIA@hq.dhs.gov

Your Component Privacy Office will submit the PTA on behalf of your office. Upon receipt from your Component Privacy Office, the DHS Privacy Office will review this form. If a PIA, SORN, or other privacy compliance documentation is required, your Component Privacy Office, in consultation with the DHS Privacy Office, will send you a copy of the template to complete and return.

For more information about the DHS Privacy compliance process, please see <https://www.dhs.gov/compliance>. A copy of the template is available on DHS Connect at <http://dhsconnect.dhs.gov/org/offices/priv/Pages/Privacy-Compliance.aspx> or directly from the DHS Privacy Office via email: [PIA@hq.dhs.gov](mailto:PIA@hq.dhs.gov) or phone: 202-343-1717.



## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project, Program, or System Name:</b>	Babel Street "BabelX" Platform		
<b>Component or Office:</b>	Customs and Border Protection (CBP)	<b>Office or Program:</b>	OFO
<b>FISMA Name (if applicable):</b>	Click here to enter text.	<b>FISMA Number (if applicable):</b>	Click here to enter text.
<b>Type of Project or Program:</b>	Pilot	<b>Project or program status:</b>	Operational
<b>Date first developed:</b>	January 1, 2018	<b>Pilot launch date:</b>	September 26, 2019
<b>Date of last PTA update</b>		<b>Pilot end date:</b>	September 25, 2023
<b>ATO Status (if applicable):<sup>1</sup></b>	Not started	<b>Expected ATO/ATP/OA date (if applicable):</b>	Click here to enter a date.

### PROJECT, PROGRAM, OR SYSTEM MANAGER

<b>Name:</b>	(b)(6) (b)(7)(C)		
<b>Office:</b>	OFO	<b>Title:</b>	(A) Director
<b>Phone:</b>	Click here to enter text.	<b>Email:</b>	SCOTT.P.FOSTER@CBP.DHS.GOV

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	Click here to enter text.		
<b>Phone:</b>	Click here to enter text.	<b>Email:</b>	Click here to enter text.

<sup>1</sup> The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see <http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/Authority%20to%20Proceed%20Memo%20Phase%20II.pdf>.



## Specific PTA Questions

### 1. Reason for submitting the PTA: New PTA

#### Background

(U//LES) U.S. Customs and Border Protection (CBP), Office of Field Operations (OFO), National Targeting Center (NTC), Counter Network Division (CND), Publicly Available Information Group (PAIG) is submitting this PTA to continue to pilot the use of Babel Street's BabelX platform. BabelX provides CBP with advanced capabilities in several areas of Publicly Available Information (PAI) and social media research which assist in mission critical CBP operations. The product is a multi-lingual, geo-enabled, text-analytics, social media and web-monitoring platform designed to meet the needs of its customers by fully leveraging PAI.

(U//LES) Babel X is an open source, intelligence monitoring web-based platform designed specifically to meet the needs of the Intelligence Community (IC) and federal law enforcement in developing Open Source Intelligence (OSINT). The platform can search for keywords and keyword combinations, phrases, hash tags, and names. It can handle requests across more than 52+ social media platforms and millions of URLs and deep/dark web data. Babel X can perform cross-lingual searches across more than 200 languages, allowing users to enter terms in English and return foreign language results. The platform also has the ability to build sophisticated filtering options for catered feeds and render various data visualizations. Lastly, Babel X allows for networks discovery with social media link analysis and provides user anonymity in viewing collected results.

(U//LES) Users can create hotlists based on events or known terms used by bad actors in order to identify derogatory information or information that may show threats to CBP and national security. A BabelX user will then review any hits to determine if information is relevant and should be retained.

(U//LES) BabelX makes sense of large tracts of multi-lingual data in near real time. Users identify themes, entities, and categories, as well as detect relationships, within the cloud based platform. Babel users can explore the data through a wide range of analytical lenses to include geospatial, temporal, link analysis, public records search, sentiment, and topics of interest.

- Built in translation of searches and search results in a wide variety of applicable languages, with a built in ontology capability;
- Easy customization and incorporation of new publically available data sets;
- Public records database capabilities;
- Powerful search capability for law enforcement targets; and

(U//LES) BabelX has the ability to create geofences so CBP can view information posted from or about certain locations only. (b) (7)(E)

(b) (7)(E)

BabelX knows location information if



## Privacy Threshold Analysis

Version number: 03-2020

Page 4 of 14

individual's have geolocation turned on for their posts. This PTA covers BabelX and not LocateX which uses AdID information to determine location. LocateX is covered by the commercial telemetry PTA.

### (U//FOUO//LES) Enhancing CBP's Targeting Enterprise

Babel data will be used/captured/stored in support of CBP targeting, vetting, operations and analysis. This will parallel already existing CBP efforts to leverage PAI. During this pilot, activities will be fluid to allow research on a range of activities and will be used to identify potential derogatory and confirmatory information associated with traveler's, persons seeking benefits, and persons of interest. CBP does not rely solely on information found in BabelX when taking actions. Relevant information would be retained as follows:

(b) (7) (E)

(U//LES) CBP will not retain PII unless the information is put into one of the above systems and linked to an individual as derogatory or to confirm information.

(U//LES) For technical help, 3 Babel Street employees have access to CBP queries, but only upon request from CBP and in an audited and access restricted "vault." BabelX stores queries forever, however it does not store results of queries.



<b>2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information?</b> <i>Please check all that apply.</i>	<input type="checkbox"/> This project does not collect, store, maintain, use, or disseminate any personally identifiable information <sup>2</sup> <input checked="" type="checkbox"/> Members of the public <input checked="" type="checkbox"/> U.S. Persons (U.S. citizens or lawful permanent residents) <input checked="" type="checkbox"/> Non-U.S. Persons <input type="checkbox"/> DHS Employees/Contractors (list Components): <i>Click here to enter text.</i> <input type="checkbox"/> Other federal employees or contractors (list agencies): <i>Click here to enter text.</i>
<b>2(a) Is information meant to be collected from or about sensitive/protected populations?</b>	<input type="checkbox"/> No <input type="checkbox"/> 8 USC § 1367 protected individuals (e.g., T, U, VAWA) <sup>3</sup> <input checked="" type="checkbox"/> Refugees/Asylees <input type="checkbox"/> Other. Please list: <i>Click here to enter text.</i>

<b>3. What specific information about individuals is collected, maintained, used, or disseminated?</b>
<p><i>Please provide a specific description of information that is collected, generated, or retained (such as names, addresses, emails, etc.) for each category of individual or population.</i></p> <p>(U//LES) Babel may assist analysts with locating and assessing the following publicly available information:</p> <p>First, Middle, Last Name Date of Birth Address</p>

<sup>2</sup> DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

<sup>3</sup> This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, available at <http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/002-02.pdf>





## Privacy Threshold Analysis

Version number: 03-2020

Page 6 of 14

Usernames  
 Email Address  
 Phone Number  
 Social Media Content  
 Images  
 IP Address Domain Information  
 Social Security Number  
 Driver's License Number  
 Employment History  
 Location data based on geolocation tags in public posts  
 AdID information is available through locateX

### 3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?<sup>4</sup> If applicable, check all that apply.

- |   |   |
|---|---|
| <input type="checkbox"/> Social Security number<br><input type="checkbox"/> Alien Number (A-Number)<br><input type="checkbox"/> Tax Identification Number<br><input type="checkbox"/> Visa Number<br><input type="checkbox"/> Passport Number<br><input type="checkbox"/> Bank Account, Credit Card, or other financial account number<br><input type="checkbox"/> Driver's License/State ID Number | <input type="checkbox"/> Social Media Handle/ID<br><input type="checkbox"/> Biometric identifiers (e.g., <i>FIN</i> , <i>EID</i> )<br><input type="checkbox"/> Biometrics. <sup>5</sup> Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.<br><input type="checkbox"/> Other. Please list: Click here to enter text. |
|---|---|

### 3(b) Please provide the specific legal basis for the collection of SSN:

(U//FOUO) CBP is proposing to obtain access to commercially available records, some of which contain social security numbers compiled by private third parties. CBP is not proposing to collect SSNs directly from individuals as part of this effort. CBP obtains access to commercially available information in furtherance of its statutory law enforcement and border security responsibilities. See, e.g., 6 U.S.C. 211; The Tariff Act of 1930, as

<sup>4</sup> Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, available at <https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information>.

<sup>5</sup> If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.



	amended; The Immigration and Nationality Act (“INA”), as amended, 8 U.S.C. § 1101, et seq
<b>3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.</b>	
<p>(U//LES) SSN is not “required” to conduct queries to fulfill the requirement of the platform. CBP will conduct social security number queries on a case by case basis and will be utilized like other selectors of interest (when available or identified through other queries). Through Babel’s partnership agreements with public and private data sources, it is able to combine PAI with identifiers such as SSNs.</p> <p>(U//LES) CBP is primarily using Babel data to lookup telephone numbers, email addresses, usernames in order to develop confirmatory or derogatory information. On occasion, when a telephone number is queried, an individual’s name, address and SSN, among others, will be returned as a result.</p>	
<b>3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, <i>SSN Collection and Use Reduction</i>,<sup>6</sup> which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.</b>	
<p>(U//FOUO) SSN is not “required” to conduct queries to fulfill the requirement of the platform. CBP will conduct social security number queries on a case by case basis and will be utilized like other selectors of interest (when available or identified through other queries).</p>	
<b>4. How does the Project, Program, or System retrieve information?</b>	<p><input checked="" type="checkbox"/> By a unique identifier.<sup>7</sup> Please list all unique identifiers used: Same as above in #3. (U//LES) Username, Email, Name, Street Address, City, State, Zip Code, Country, Social Security Number, Driver’s License Number, Domain Name, IP Address, telephone number</p> <p><input checked="" type="checkbox"/> By a non-unique identifier or other means. Please describe:</p>

<sup>6</sup> See <https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction>.

<sup>7</sup> Generally, a unique identifier is considered any type of “personally identifiable information,” meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



	(U//LES) BabelX users can create geofences for publicly available geotagged social media content.
<p><b>5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? If no schedule has been approved, please provide proposed schedule or plans to determine it.</b></p> <p><i>Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.<sup>8</sup></i></p>	<p>(U//FOUO) For queries conducted in BabelX, those queries will be stored within Babel forever. The results of those queries are not saved or retained by the vendor. Access to individual account search queries is accessed/maintained by the vendors Director of Technology for auditing purposes. The vendor is currently creating an Administrator Module where an assigned CBP administrator will be able to review individual queries conducted by any CBP user for auditing purposes. The results/findings/analysis of queries conducted by CBP operators and analysts will be maintained in approved CBP Systems of Record such as Automated Targeting System (ATS), Analytical Framework for Intelligence (AFI), Intelligence Reporting System –Next Generation (IRS-NG), and/or TECS for 75 years.</p>
<p><b>5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)?</b></p>	<p>(U//FOUO) For queries conducted in BabelX, those queries will be stored within BabelX forever. The results of those queries are not saved or retained by the vendor. Access to individual account search queries is accessed/maintained by the vendor's Director of Technology for auditing purposes. CBP program manager gets monthly reports from the Vendor on usage statistics and can request audit logs for any CBP accounts as appropriate for auditing purposes. The results/findings/analysis of queries conducted by CBP operators and analysts will be maintained in approved CBP Systems of Record.</p>
<p><b>6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?<sup>9</sup></b></p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please list:</p>

<sup>8</sup> See <http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/IS2O/rm/Pages/RIM-Contacts.aspx>

<sup>9</sup> PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in IACS.





<b>7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list:  This is a commercial entity that shares with other U.S. government agencies.
<b>8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? If applicable, please provide agreement as an attachment.</b>	Choose an item.  Please describe applicable information sharing governance in place: <i>Click here to enter text.</i>
<b>9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?</b>	<input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: <i>Click here to enter text.</i> <input type="checkbox"/> Yes. In what format is the accounting maintained: <i>Click here to enter text.</i>
<b>10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:</b>	<input checked="" type="checkbox"/> Social Media <input type="checkbox"/> Advanced analytics <sup>10</sup> <input type="checkbox"/> Live PII data for testing <input type="checkbox"/> No

<sup>10</sup> The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.



<p><b>11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?<sup>11</sup> This does not include subject-based searches.</b></p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i></p>
<p><b>11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?</b></p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i></p>
<p><b>12. Does the planned effort include any interaction or intervention with human subjects<sup>12</sup> via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for <u>research purposes</u></b></p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for <u>independent</u> review and approval of this effort.<sup>13</sup></p>
<p><b>13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, <u>in addition</u> to annual privacy training required of all DHS personnel?</b></p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list: CBP personnel using the database are required to act in accordance with CBP's existing authorities and in compliance with the CBP Social Media Directive (including completing the required training) and Social Media Rules of Behavior.</p>

<sup>11</sup> Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program; or

(ii) the security of a Government computer system.

<sup>12</sup> Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

<sup>13</sup> For more information about CAPO and their points of contact, please see: <https://www.dhs.gov/publication/compliance-assurance-program-office> or <https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36>. For more information about the protection of human subjects, please see DHS Directive 026-04: [https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir\\_026-04-protection-of-human-subjects\\_revision-01.pdf](https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf).



## Privacy Threshold Analysis

Version number: 03-2020

Page 11 of 14

<b>14. Is there a FIPS 199 determination?<sup>14</sup></b>	<input checked="" type="checkbox"/> No.  <input type="checkbox"/> Yes. Please indicate the determinations for each of the following:  Confidentiality: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Integrity: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Availability: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	--

## PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	(b)(6) (b)(7)(C)
<b>Date submitted to Component Privacy Office:</b>	<i>Click here to enter a date.</i>
<b>Concurrence from other Component Reviewers involved (if applicable):</b>	<i>Click here to enter text.</i>
<b>Date submitted to DHS Privacy Office:</b>	November 17, 2020
<b>Component Privacy Office Recommendation:</b> <i>Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.</i>	
(b) (5)	

<sup>14</sup> FIPS 199 is the [Federal Information Processing Standard](#) Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.



(b) (5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6) (b)(7)(C)
DHS Privacy Office Approver (if applicable):	<a href="#">Click here to enter a date.</a>
Workflow Number:	<a href="#">Click here to enter text.</a>
Date approved by DHS Privacy Office:	December 14, 2020
PTA Expiration Date	September 25, 2023

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	System If "other" is selected, please describe: <a href="#">Click here to enter text.</a>
Determination:	<input checked="" type="checkbox"/> Project, Program, System in compliance with full coverage <input type="checkbox"/> Project, Program, System in compliance with interim coverage <input type="checkbox"/> Project, Program, System in compliance until changes implemented <input type="checkbox"/> Project, Program, System not in compliance
PIA:	<b>System covered by existing PIA</b> DHS/CBP/PIA-058 Publicly Available Social Media Monitoring and Situational Awareness Initiative; DHS/CBP/PIA-007 ESTA; DHS/CBP/PIA-009 TECS; DHS/CBP/PIA-006 ATS; Forthcoming IRS-NG and Trusted Traveler Programs PIAs
SORN:	System covered by existing SORN DHS/CBP-002 Trusted and Registered Traveler Programs, March 11, 2020, 85 FR 14214; DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297;



	DHS/CBP-009 Electronic System for Travel Authorization (ESTA); DHS/CBP-011 U.S. Customs and Border Protection TECS; DHS/CBP-024 Intelligence Records System (CIRS) System of Records
--	--

**DHS Privacy Office Comments:**

*Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.*

(U//LES) CBP is submitting this PTA to discuss a pilot of Babel Street's BabelX platform, which is an open source, intelligence monitoring web-based platform that will provide CBP with advanced capabilities in several areas of Publicly Available Information (PAI) and social media research to assist in mission critical CBP operations.

(U//LES) The platform can perform cross-lingual searches (i.e., entering English search terms and returning foreign language results) for keywords and keyword combinations, phrases, hashtags, and names across 52+ social media platforms and millions of URLs and deep/dark web data. The platform can also build filtering options for catered feeds and render various data visualizations. Users can identify themes, entities, and categories, as well as detect relationships, and can explore the data through a wide range of analytical lenses such as geospatial, temporal, link analysis, public records search, sentiment, and topics of interest.



The DHS Privacy Office agrees this pilot is privacy sensitive and requires PIA coverage. As BabelX will be used for a variety of specific targeting and vetting operations and analysis, coverage is dependent on the specific use of the tool. Social media monitoring and situational awareness is covered by DHS/CBP/PIA-058 Publicly Available Social Media Monitoring and Situational Awareness Initiative. Coverage for various vetting and targeting activities is provided by DHS/CBP/PIA-007 Electronic System for Travel Authorization (ESTA), DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, DHS/CBP/PIA-006 Automated Targeting System (ATS), as well as the forthcoming IRS-NG and Trusted Traveler Program PIAs.

SORN coverage is also required and is provided by DHS/CBP-006 ATS, DHS/CBP-002 Trusted and Registered Traveler Programs, DHS/CBP-011 U.S. Customs and Border Protection TECS, DHS/CBP-009 Electronic System for Travel Authorization (ESTA), and DHS/CBP-024 Intelligence Records System (CIRS) System of Records.





# Homeland Security

Privacy Office

U S Department of Homeland Security

Washington, DC 20528

202-343-1717, pia@hq.dhs.gov

[www.dhs.gov/privacy](http://www.dhs.gov/privacy)

**Privacy Threshold Analysis**

**Version number: 03-2020**

*Page 14 of 14*